UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/582,143	03/27/2007	Martin Paul Moshal	06-408	8831

20306 7590 12/07/2010

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER	
MYHR, JUSTIN L	

ART UNIT	PAPER NUMBER
3714	

MAIL DATE	DELIVERY MODE
12/07/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/582,143	MOSHAL, MARTIN PAUL	
	Examiner	Art Unit	
	JUSTIN MYHR	3714	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 September 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-88* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-88* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/22/2010*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to amendments filed on 9/29/2010.

Claim Objections

2. Claim 23 is objected to because of the following informalities: Item "software-" should be recited as --software--, so as to clarify the confusion. Appropriate correction is required.

3. Claim 77 objected to because of the following informalities: Item "one-to-ore" should be recited as --one to one--, so as to clarify the confusion. Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claims 1, 3-16, 18, 21-24, 28-44, and 48-60, 62-84, and 86-88 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mott et al. (US Pat. No. 6,170,060 B1 hereinafter referred to as Mott) in view of Nguyen et al. (US Pub. No. 2002/0116615 A1 hereinafter referred to as Nguyen).

As per claim 1, Mott teaches a processor module for a player station operable by a player (abstract), comprising: a processor (Fig. 1); a storage memory accessible by the processor (Fig. 1); an interface facility communicable with the processor and with at least one peripheral device (Fig. 1); a unique identification code associated with the processor module (col. 2, lines 9-14 and col. 12, lines 19-29 device ID); and a security module co-operable with the processor, the security module being arranged to decrypt an encrypted software program (col. 8, lines 26-34 and col. 14, lines 3-11 in one embodiment the software program is encrypted using a known key) to recover an identification code therefrom, to enable execution of the software program by the processor to execute the program when the recovered identification code matches the unique identification code associated with the processor module, and to disable execution of the software program when the recovered identification code does not match the unique identification code associated with the processor module (Fig. 12 and col. 5, lines 50-51, col. 8, lines 26-34, col. 9, lines 37-39, col. 10, lines 13-16, col. 14, lines 3-14, and col. 18, lines 28-36 device is designed to provide a program file, which could include software code, to a player and include within the program file a unique ID associated with the device. Once decrypted the device confirms that the ID matches its

own and will execute the program only when it does.). Mott does not specifically teach that the device or the program is related to gaming. However, Nguyen teaches providing a secure system for the purpose of downloading a game program from a first machine to a second machine for the purposes of the second machine running the game (abstract and Fig. 14). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Mott with Nguyen, since Mott is modifiable to be used in the gaming art since it is desired in the game art to provide a secure and easy manner of downloading and installing games on a authorized gaming machine (Nguyen paragraph [0016]).

As per claim 3, Mott does not specifically teach a processor module in which the unique identification code is stored in a protected area of the storage memory. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made that the storage medium storing the unique identification code would have to be a protected area in order to insure that no tampering is done with the device identification code since this would negate the system of Mott in which each identification code is unique to that device.

As per claim 4, Mott does not specifically teach a processor module in which the protected area of the storage memory is a read-only memory. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made that the storage medium storing the unique identification code would have to be a protected area in order to insure that no tampering is done with the device identification code

since this would negate the system of Mott in which each identification code is unique to that device.

As per claim 5, Mott teaches a processor module in which the interface facility is an input/output circuit connected to the processor by means of an input/output bus (Fig. 1).

As per claim 6, Mott teaches a processor module in which the at least one peripheral device is any one of a display monitor, a magnetic card reader, a banknote validator, an array of pushbuttons, a coin acceptor, a ticket reader, a numeric keypad, a printer and a counter (Fig. 1).

As per claim 7, Mott does not specifically teach a processor module in which communication between the processor and the at least one peripheral device is encrypted. However, it is old and well known in the art at the time the invention was made to encrypt the communication between peripheral devices for security purposes.

As per claim 8-9, Mott does not teach a processor module in which the processor module includes a random number generator and in which the random number generator is a hardware random number generator. However, it is old and well known in the art at the time the invention was made to include hardware based random number generators in order to produce random outcomes.

As per claim 10, Mott teaches a processor module in which the storage memory includes a still further portion that is removable (Fig. 1).

As per claim 11, Mott teaches a processor module in which the removable portion of the storage memory is a flash memory module (co. 17, lines 40-45).

As per claim 12, Mott teaches a processor module in which the processor includes a network interface that provides access to a communication network (Fig. 1).

As per claim 13, Mott teaches a processor module in which the communication network is the Internet (col. 4, lines 45-47).

As per claims 14 and 15, Mott teaches a processor module in which the processor module also includes a number of interface ports and in which the number of interface ports include any one or more of a serial communication port and a port conforming to the Universal Serial Bus standard (col. 3, lines 57-60).

As per claim 16, Mott teaches a processor module method for configuring a processor module for a player station operable by a player thereon (abstract), comprising the steps of: obtaining a unique identification code associated with the processor module (col. 2, lines 9-14 and col. 12, lines 19-29 device ID); encrypting a software program remotely from the processor module as a function of the unique identification code (col. 13, lines 29-36); transferring the encrypted software program to the processor module (abstract); decrypting the encrypted software program to obtain a decrypted identification code therefrom (Fig. 12 and col. 5, lines 50-51, col. 8, lines 26-34, col. 9, lines 37-39, col. 10, lines 13-16, col. 14, lines 3-14, and col. 18, lines 28-36 device is designed to provide a program file, which could include software code, to a player and include within the program file a unique ID associated with the device. Once decrypted the device confirms that the ID matches its own and will execute the program only when it does.); and configuring the processor module to enable execution of the encrypted software program by the processor module when the decrypted identification

code is the same as the unique identification code of the processor module and configuring the processor module to disable execution of the encrypted software program by the processor module when the decrypted identification code is different from the unique identification code of the processor module (Fig. 12 and col. 5, lines 50-51, col. 8, lines 26-34, col. 9, lines 37-39, col. 10, lines 13-16, col. 14, lines 3-14, and col. 18, lines 28-36 device is designed to provide a program file, which could include software code, to a player and include within the program file a unique ID associated with the device. Once decrypted the device confirms that the ID matches its own and will execute the program only when it does.). Mott does not specifically teach that the device or the program is related to gaming. However, Nguyen teaches providing a secure system for the purpose of downloading a game program from a first machine to a second machine for the purposes of the second machine running the game (abstract and Fig. 14). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Mott with Nguyen, since Mott is modifiable to be used in the gaming art since it is desired in the game art to provide a secure and easy manner of downloading and installing games on a authorized gaming machine (Nguyen paragraph [0016]).

As per claim 18, Mott does not specifically teach a method in which the unique identification code is stored in a protected area of the storage memory. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made that the storage medium storing the unique identification code would have to be a protected area in order to insure that no tampering is done with the device identification

code since this would negate the system of Mott in which each identification code is unique to that device.

As per claim 21, Mott teaches a method that includes a step of jointly encrypting a plurality of different software programs remotely from the processor module as a function of the unique identification code, each one of the plurality of software programs being executable (ordering more then one).

As per claim 22, Mott teaches a method in which the jointly encrypted plurality of software programs are transferred to the processor module (abstract).

As per claim 23, Mott teaches a method in which the jointly encrypted plurality of software programs are decrypted to obtain a decrypted identification code therefrom, and execution of any selected one of the jointly encrypted plurality of software programs is enabled when the decrypted identification code is the same as the unique identification code of the processor module, and execution of all of the jointly encrypted plurality of software programs is disabled when the decrypted identification code is different from the unique identification code of the processor module Fig. 12 and col. 5, lines 50-51, col. 8, lines 26-34, col. 9, lines 37-39, col. 10, lines 13-16, col. 14, lines 3-14, and col. 18, lines 28-36 device is designed to provide a program file, which could include software code, to a player and include within the program file a unique ID associated with the device. Once decrypted the device confirms that the ID matches its own and will execute the program only when it does.).

As per claims 24 and 44, Mott teaches a system or method for customisation and distribution of software (abstract and col. 5, lines 50-51), comprising: a number of

stations each station being associated with a unique identification code (col. 2, lines 9-14 and col. 12, lines 19-29 device ID); a repository containing a number of different software programs, each software program being executable by at least one of the number of stations (abstract); a download server communicable with the repository (Fig. 2, item 260); a communication network enabling communication between the download server and each one of the number of player stations (Fig. 2); encryption means operable to encrypt, remotely from the number of player stations, a selectable one of the number of different software programs contained in the repository as a function of the unique identification code of a selectable one of the number of player stations, the download server being responsive to the encryption means to download the encrypted software program to the particular player station whose unique identification code was used for encryption (col. 13, lines 29-36); and a security module associated with the particular player station, the security module being capable of decrypting the downloaded encrypted software program to obtain therefrom a decrypted identification code and enabling execution of the downloaded encrypted software program by the particular player station when the decrypted identification code is the same as the unique identification code of the particular player station, and disabling execution of the downloaded encrypted software program by the particular player station when the decrypted identification code is different from the unique identification code of the particular player station (Fig. 12 and col. 5, lines 50-51, col. 8, lines 26-34, col. 9, lines 37-39, col. 10, lines 13-16, col. 14, lines 3-14, and col. 18, lines 28-36 device is designed to provide a program file, which could include software code, to a player and

include within the program file a unique ID associated with the device. Once decrypted the device confirms that the ID matches its own and will execute the program only when it does.). Mott does not specifically teach that the device or the program is related to gaming. However, Nguyen teaches providing a secure system for the purpose of downloading a game program from a first machine to a second machine for the purposes of the second machine running the game (abstract and Fig. 14). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Mott with Nguyen, since Mott is modifiable to be used in the gaming art since it is desired in the game art to provide a secure and easy manner of downloading and installing games on a authorized gaming machine (Nguyen paragraph [0016]).

As per claims 28 and 48, Mott teaches a system or method that includes a step of jointly encrypting a plurality of different software programs remotely from the processor module as a function of the unique identification code, each one of the plurality of software programs being executable (ordering more then one).

As per claims 29 and 49, Mott teaches a system or method in which the jointly encrypted plurality of software programs are transferred to the processor module (abstract).

As per claims 30 and 50, Mott teaches a system or method in which the jointly encrypted plurality of software programs are decrypted to obtain a decrypted identification code therefrom, and execution of any selected one of the jointly encrypted plurality of software programs is enabled when the decrypted identification code is the

same as the unique identification code of the processor module, and execution of all of the jointly encrypted plurality of software programs is disabled when the decrypted identification code is different from the unique identification code of the processor module Fig. 12 and col. 5, lines 50-51, col. 8, lines 26-34, col. 9, lines 37-39, col. 10, lines 13-16, col. 14, lines 3-14, and col. 18, lines 28-36 device is designed to provide a program file, which could include software code, to a player and include within the program file a unique ID associated with the device. Once decrypted the device confirms that the ID matches its own and will execute the program only when it does.).

As per claim 31, Mott teaches a system in which each player station has an associated storage memory (Fig. 1).

As per claims 32 and 51, Mott does not specifically teach a system or method in which the unique identification code is stored in a protected area of the storage memory. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made that the storage medium storing the unique identification code would have to be a protected area in order to insure that no tampering is done with the device identification code since this would negate the system of Mott in which each identification code is unique to that device.

As per claim 33, Mott does not specifically teach a system in which the protected area of the storage memory is a read-only memory. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made that the storage medium storing the unique identification code would have to be a protected area in order to insure that no tampering is done with the device identification code

since this would negate the system of Mott in which each identification code is unique to that device.

As per claim 34, Mott teaches a system in which each player station includes a processor and a number of peripheral devices (Fig. 1).

As per claim 35, Mott teaches a system in which the at least one peripheral device is any one of a display monitor, a magnetic card reader, a banknote validator, an array of pushbuttons, a coin acceptor, a ticket reader, a numeric keypad, a printer and a counter (Fig. 1).

As per claim 36, Mott does not specifically teach a system in which communication between the processor and the at least one peripheral device is encrypted. However, it is old and well known in the art at the time the invention was made to encrypt the communication between peripheral devices for security purposes.

As per claim 37-38, Mott does not teach a system in which the processor module includes a random number generator and in which the random number generator is a hardware random number generator. However, it is old and well known in the art at the time the invention was made to include hardware based random number generators in order to produce random outcomes.

As per claim 39, Mott teaches a system in which the storage memory includes a still further portion that is removable (Fig. 1).

As per claim 40, Mott teaches a system in which the removable portion of the storage memory is a flash memory module (co. 17, lines 40-45).

As per claim 41, Mott teaches a system in which the communication network is the Internet (col. 4, lines 45-47).

As per claims 42 and 43, Mott teaches a system in which the processor module also includes a number of interface ports and in which the number of interface ports include any one or more of a serial communication port and a port conforming to the Universal Serial Bus standard (col. 3, lines 57-60).

As per claims 52 and 76, Mott teaches a system or method for the distribution of software (abstract and col. 5, lines 50-51), comprising: a repository containing a number of different executable software programs (abstract, Fig. 2, and col. 5, lines 50-51); a download server communicable with the repository (Fig. 2, item 260); a number of processor modules, each processor module being identified by means of a unique identification code and being operable to execute any one of the number of different software programs contained in the repository (Fig. 2); receiving means for receiving a request to execute a desired combination of at least one software program contained in the repository on at least one of the number of processor modules, the request containing at least one selectable identification code-to-software program mapping (Figs. 1-2 and 12 and col. 5, lines 50-51, col. 8, lines 26-34, col. 9, lines 37-39, col. 10, lines 13-16, col. 14, lines 3-14, and col. 18, lines 28-36 user wishes to use the program); encryption means to encrypt the particular software program contained in the at least one selectable mapping as a function of the identification code in the mapping (col. 13, lines 29-36); a download facility operable to download the encrypted particular software program to the particular processor module whose identification code was

used for encryption (Fig. 2, item 260); and a security module associated with the particular processor module, the security module being capable of decrypting the downloaded encrypted software program to obtain therefrom a decrypted identification code and enabling execution of the downloaded encrypted software program by the particular processor module when the decrypted identification code is the same as the unique identification code of the particular processor module, and disabling execution of the downloaded encrypted software program by the particular processor module when the decrypted identification code is different from the unique identification code of the particular processor module (Fig. 12 and col. 5, lines 50-51, col. 8, lines 26-34, col. 9, lines 37-39, col. 10, lines 13-16, col. 14, lines 3-14, and col. 18, lines 28-36 device is designed to provide a program file, which could include software code, to a player and include within the program file a unique ID associated with the device. Once decrypted the device confirms that the ID matches its own and will execute the program only when it does.). Mott does not specifically teach payment means for receiving a fee for the requested licence. However, Nguyen does teach providing a secure system for downloading a game program and for purchasing a license for a piece of gaming software on the machine (Figs. 6-7). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Mott with Nguyen, since Mott is modifiable to include methods of billing for software purchases so as to raise revenue for the software developer and distributor.

As per claims 53 and 77, Mott does not specifically teach a system or method in which the at least one selectable mapping is a one-to-one mapping. However, Nguyen

does teach a system in which the at least one selectable mapping is a one-to-one mapping (paragraph [0099]). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Mott with Nguyen, since Mott is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claims 54 and 78, Mott does not specifically teach a system or method in which the license request contains a plurality of different one-to-one mappings, each unique processor module identification code being contained in only one such mapping. However, Nguyen does teach a system in which the license request contains a plurality of different one-to-one mappings, each unique processor module identification code being contained in only one such mapping (Figs. 6-7 and paragraph [0099] able to purchase multiple licenses depending on need). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Mott with Nguyen, since Mott is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claims 55 and 79, Mott does not specifically teach a system or method in which the encryption means is responsive to payment of the fee to encrypt the particular software program contained in each one of the plurality of different one-to-one mappings as a function of the identification code in that mapping. However, it would

have been obvious to one of ordinary skill in the art that Mott would require the software to be purchased first before allowing a user to download it since the key needed to decrypt the software is already present on the system.

As per claims 56 and 80, Mott teaches a system or method in which the download facility downloads each encrypted software program to the particular processor module whose identification code was used for encryption (col. 13, lines 29-36).

As per claims 57 and 81, Mott does not specifically teach a system or method in which the at least one selectable mapping is a many-to-one mapping. However, Nguyen does teach a system in which the at least one selectable mapping is a many-to-one mapping (Figs. 6-7 and paragraph [0078] can purchase a license for multiple games and paragraph [0133] allows for multiple gaming machines per license). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Mott with Nguyen, since Mott is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claims 58 and 82, Mott does not specifically teach a system or method each unique processor module identification code being contained in only one such mapping. However, Nguyen does teach a system in which the at least one selectable mapping is a many-to-one mapping (Figs. 6-7 and paragraph [0078] can purchase a license for multiple games and paragraph [0133] allows for multiple gaming machines

per license) and Mott teaches encrypting the download using the gaming machines unique code (col. 13, lines 29-36). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Mott with Nguyen, since Mott is modifiable to allow the purchase of licenses which enable a single gaming machine to run the downloaded game thereby saving the operator time since they do not need to go through the hassle of purchasing the license separately.

As per claims 59 and 83, Mott does not specifically teach a system or method in which the encryption means is responsive to payment of the fee to encrypt the particular software program contained in each one of the different many-to-one mappings with each one of the plurality of identification codes in that mapping to obtain separate encrypted instances of the same software program. However, it would have been obvious to one of ordinary skill in the art that Mott would require the software to be purchased first before allowing a user to download it since the key needed to decrypt the software is already present on the system.

As per claims 60 and 84, Mott teaches a system or method in which the download facility downloads each encrypted software program to the particular processor module whose identification code was used for encryption (col. 13, lines 29-36).

As per claim 62, Mott teaches a system in which each player station has an associated storage memory (Fig. 1).

As per claims 63 and 86, Mott does not specifically teach a system or method in which the unique identification code is stored in a protected area of the storage memory. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made that the storage medium storing the unique identification code would have to be a protected area in order to insure that no tampering is done with the device identification code since this would negate the system of Mott in which each identification code is unique to that device.

As per claim 64, Mott does not specifically teach a system in which the protected area of the storage memory is a read-only memory. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made that the storage medium storing the unique identification code would have to be a protected area in order to insure that no tampering is done with the device identification code since this would negate the system of Mott in which each identification code is unique to that device.

As per claims 65 and 87, Mott teaches a system or method in which each player station includes a processor and a number of peripheral devices (Fig. 1).

As per claim 66, Mott teaches a system in which the at least one peripheral device is any one of a display monitor, a magnetic card reader, a banknote validator, an array of pushbuttons, a coin acceptor, a ticket reader, a numeric keypad, a printer and a counter (Fig. 1).

As per claims 67 and 88, Mott does not specifically teach a system in which communication between the processor and the at least one peripheral device is

encrypted. However, it is old and well known in the art at the time the invention was made to encrypt the communication between peripheral devices for security purposes.

As per claim 68-69, Mott does not teach a system in which the processor module includes a random number generator and in which the random number generator is a hardware random number generator. However, it is old and well known in the art at the time the invention was made to include hardware based random number generators in order to produce random outcomes.

As per claim 70, Mott teaches a system in which the storage memory includes a still further portion that is removable (Fig. 1).

As per claim 71, Mott teaches a system in which the removable portion of the storage memory is a flash memory module (co. 17, lines 40-45).

As per claim 72-73, Mott teaches a system in which the communication network is the Internet (col. 4, lines 45-47).

As per claims 74 and 75, Mott teaches a system in which the processor module also includes a number of interface ports and in which the number of interface ports include any one or more of a serial communication port and a port conforming to the Universal Serial Bus standard (col. 3, lines 57-60).

8. Claims 2, 17, 25, 45, 61 and 85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mott et al. (US Pat. No. 6,170,060 B1 hereinafter referred to as Mott) and Nguyen et al. (US Pub. No. 2002/0116615 A1 hereinafter referred to as Nguyen) in view of Hashimoto et al. (US Pub. No. 2002/0053024 A1 hereinafter referred to as Hashimoto).

As per claims 2, 17, 25, 45, 61 and 85, Mott does not specifically teach a processor in which the security module also disables execution of the software program when the software program is unencrypted. However, Hashimoto does teach insuring that illegal analysis and tampering of programs does not occur by use of software encryption (paragraphs [0007]-[0008]). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Mott and Nguyen with Hashimoto since Mott is modifiable to use the system of Hashimoto to prevent software tampering by preventing unencrypted software from running since the purpose of Hashimoto is to have a processor which processes encrypted software in order to prevent illegal use and this purpose is not fulfilled if the software is not encrypted.

9. Claims 19-20, 26-27, and 46-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mott et al. (US Pat. No. 6,170,060 B1 hereinafter referred to as Mott) and Nguyen et al. (US Pub. No. 2002/0116615 A1 hereinafter referred to as Nguyen) in view of Reeder (US Pat. No. 6,141,652).

As per claims 19, 26, and 46, Mott does not specifically teach a method in which execution of the encrypted software program is enabled for a predetermined period of time. However, Reeder does teach a method in which execution of the encrypted software program is enabled for a predetermined period of time (col. 7, lines 16-30 renting software). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Mott with Nguyen and Reeder, since Mott is modifiable to include support for rentable software in which

validation is sought after a set amount of time in order to allow a gaming machine to continue executing the game after confirming with the provider that the copy is still valid.

As per claims 20, 27, and 47, Mott does not specifically teach a method in which execution of the encrypted software program is re-enabled upon the occurrence of a predetermined event. However, Reeder does teach a method in which execution of the encrypted software program is re-enabled upon the occurrence of a predetermined event (col. 7, lines 16-30 renting software). Hence, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teachings of Mott with Nguyen and Reeder, since Mott is modifiable to include support for rentable software in which validation is sought after a set amount of time in order to allow a gaming machine to continue executing the game after confirming with the provider that the copy is still valid.

Response to Arguments

10. Applicant's arguments with respect to claims 1-88 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JUSTIN MYHR whose telephone number is (571)270-7847. The examiner can normally be reached on Monday-Thursday 7:30 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Lewis can be reached on (571)272-7673. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JUSTIN MYHR/

Examiner, Art Unit 3714

12/02/2010

/Ronald Laneau/
Primary Examiner, Art Unit 3714